REMARKS

Applicants appreciate the Examiner's thorough examination of the subject application and request reconsideration of the subject application based on the foregoing amendments and the following remarks.

Claims 1-6 and 8-22 are pending in the subject application.

Claim 7 was previously canceled.

Claims 1-6 and 8-22 stand rejected under 35 U.S.C. §103.

Claims 1, 17 and 18 were amended for clarity and to more distinctly claim Applicants' invention.

The amendments to the claims are supported by the originally filed disclosure.

35 U.S.C. §103 REJECTIONS

Claims 1-6 and 8-22 stand rejected under 35 U.S.C. §103 as being unpatentable over the cited prior art for the reasons provided on pages 2-9 of the above referenced Office Action. Applicants respectfully traverse as discussed below. Because claim(s) was/were amended in the instant amendment, the following discussion refers to the language of the amended claims. However, only those amended features specifically relied upon to distinguish the claimed invention from the cited prior art shall be considered as being made to overcome the cited reference. The following addresses the specific rejections provided in the above-referenced Office Action.

CLAIMS 1-6, 8-14, 17-22

Claims 1-6, 8-14 and 17-22 stand rejected as being unpatentable over Burns et al. [USP 6,405,315; "Burns"] and further in view of Flyntz [US Patent Application Publication 2002/0147924] in view of "Windows 2000 Quick Fixes("Boyce") for the reasons provided on pages 2-10 of the above-identified Office Action. Applicants respectfully traverse.

The electronic network device of claim 1, includes (*inter alia*)

(a) an electronic device for transmitting data via a network;

(b) a plurality of storing means for storing data transmitted from the electronic device;

(c) a plurality of external devices for acquiring data from the storing means and processing the acquired data;

(d) a setting section for setting a security level for the data to be transmitted, wherein the security level is set in the setting section responsive to an input from a user of the electronic device, where the set security level being selected by the user is selected from a plurality of identified security levels;

(e) a network connecting the electronic device, the plurality of storing means, and the plurality of external devices to one another;

(f) the electronic device, at least one of the plurality of storing means, and at least one of the plurality of external devices each have a security function and another security level associated with the set security level;

(g) a search means for searching the plurality of storing means and for searching the plurality of external devices to identify one or more given storing means or one or more given external devices whose security level corresponds to the security level set in the setting section;

(h) a selecting means for providing results of the searching to the user and for providing an output, the output corresponding to a selected one of the identified one or more given storing means or the identified one or more given external device whose security level corresponds to the security level set in the setting section, the selected one being selected by the user from the provided search results; and

(i) the electronic device transmits the data to the selected one of the given storage means or the given external device responsive to said output from the selecting means.

In other words the electronic network device of claim 1, (1) the user sets a security level from a plurality of such security levels for the data to be transmitted, (2) a search is made to identify those storing means and external devices that whose security level corresponds to the security level set in the setting section, (3) the results of the searching are provided to the user

who selects one of the storing means and external devices that were identified in (2) and after the user selects the one, the electronic network device transmits the data to the selected one. Thus, the electronic device of claim 1 is configured and arranged so that the user provides inputs at different times which inputs are utilized to control the electronic network device. In this way, the user can send the data to a particular storage device or external device that has a desired security level. As indicated above, claim 1 was amended herein to provide that at least one of the plurality storing means has a security level that is different from another of the plurality of storing means.

In contrast to the present invention, Burns describes a decentralized remotely encrypted file system, the described system includes a plurality of storage devices which serve as a repository of the system's data. As also described in Burns, the data is encrypted by the network clients before it is sent to a storage device and the data read from the storage device is decrypted by the network client. In other words, and as previously indicated by Applicants (and admitted by the Examiner), the storage devices in Burns all have the same security level.

In the Office Action it is asserted that the storage devices have a security function and a security level. In support of the rejection, reference is made to the discussion in col. 5 that encrypted data is stored in the storage device.

It is clear that while encrypted data is being stored in the storage device in Burns, the storage device in Burns does not have a security function as that term is used in the subject application and the claims. As provided in the claim and the discussions in the subject application, security function and security level are used to describe the capability of the storage device to protect the data that is being stored in the storage device. In contrast to Burns, the security function, namely the encryption of data is performed in the client computer. This is abundantly clear from Fig. 3 in Burns which clearly shows the key and lock managers being operably coupled to the client computer.

Also the reference to the discussion in lines 25-45 in col. 5, as the sole basis upon which a storage device is asserted as having a security function also fails to be reconciled with the later discussion in Burns that asserts the opposite. As can be seen from the below excerpt (see col. 5,

ll. 47-50) the storage device in Burns is only trusted to store the encrypted data it is NOT trusted to keep the any data stored in the storage device secret.

> In the file system of the invention, a network storage device is trusted to store the encrypted file system data (not sent back old or garbage data), but it is not trusted to keep the data secret."

If one considers solely for sake of argument that a storage device having no security is representative of a security level of sorts, it is clear that all of the storage devices in Burns have the same level of security - none trusted security level. Thus, it cannot be said that at least one of the storage devices has a different security level from another storage device.

It also appears that reliance is made to Fig. 7 in the grounds for rejection as teaching a search means "for searching the plurality of storing means and for searching the plurality of external devices to identify one or more given storing means or one or more given external devices whose security level corresponds to the security level set in the setting section." As described in Burns, Fig. 7 is a flow chart showing a general sequence for the Lookup operation, for looking up a directory entry in the file system. As is known to those skilled in the art, a lookup operation for a directory entry does not describe a process for locating a storage device having a security function and security level.

As in known those skilled in the art, the administrator of a network typically performs a number of operations when initially connecting a computer to a network. This includes assigning or mapping network locations of storage devices connected to the network where data from a computer connected to the network would be stored when using an applications program being executed on the computer. This is done so that storage is done seamlessly as to the user. Otherwise a user would generally store a file to a local drive of the computer. Other actions that can be undertaken by the network administrator includes the creation of access lists or permissions that would be stored in a server accessible to the network so as to control access to the server by specific users or user groups. These operations by a network administrator hardly correspond to the searching means as set forth in the claims.

As to the assertion that Burns describes in col. 9, ll. 1-25 a setting section for setting a

security level and that the set security level is selected by the user from a plurality of security levels, as previously indicated by Applicants, this discussion in Burns (which starts in col. 8) describes the well known process for locking for cache consistency. This process does not involve setting a security level or selecting a security level from a plurality of available levels. The described process is undertaken by an operating system to prevent a user from writing to a file while another user also is writing to the same file or reading a file when another is writing to the file.

As to the newly identified reference, Boyce, it is asserted that this reference allegedly teaches that searching for storing means and external devices as set forth in the present invention is found in section 8.7.1 of Boyce. Applicants respectfully disagree.

The searching described in section 8.7.1 of Boyce is searching responsive to input of the name of a computer by a user, for a user whose name corresponds to the inputted name of the computer. Boyce does not describe, teach or suggest; searching, responsive to selection of a security level by a user, for storing means or external devices whose security level corresponds to the selected security level.

In sum, the three references alone or in combination do not describe the claimed electronic device network system of claim 1.

Also, if the system described in Burns was modified so as to yield a system as claimed by Applicants such a system would defeat the purpose and intended function of the system described in Burns. As described in Burns, the security function of encrypting data is carried out by the client computer so that the data being communicated to the storage device is encrypted so that even if the data is somehow intercepted, the data is unable to be read by the person intercepting the communication. As also described in Burns, if a storage device (hard disk) with un-encrypted data thereon was removed from the computer then the hard disk could be installed in another computer and the data retrieved from the hard disk. As the data is encrypted in the client computer in Burns, then even if the hard disk was installed in another computer the encrypted data could not be read. Thus, if the storage device in Burns was modified so that it was the only device encrypting data, then the intended operation and function of the system described in Burns

would be destroyed.

As to claims 2-6 and 8-14, each of these claims depends (directly or ultimately) from claim 1. Thus, each of claims 2-6 and 8-14 are considered to be allowable at least because of their dependency from an allowable base claim. This shall not; however, be considered an admission that claims 2-6 and 8-14 are not separately patentable from the identified combination of references.

As to claim 17, Applicants respectfully submit that the above remarks regarding claim 1, apply to distinguish the data receiver search system of claim 17 from the identified combination of references. This shall not, however, be considered an admission that there are not additional grounds for distinguishing claim 17 from the identified combination of references.

As to claim 18, Applicants respectfully submit that the above remarks regarding claim 1 apply to distinguish the data receiver search method of claim 18 from the identified combination of references. This shall not, however, be considered an admission that there are not additional grounds for distinguishing claim 18 from the identified combination of references.

As to claims 19-22, each of these claims depends (directly or ultimately) from claim 18. Thus, each of claims 19-22 are considered to be allowable at least because of their dependency from an allowable base claim. This shall not; however, be considered an admission that claims 19-22 are not separately patentable from the identified combination of references.

It is respectfully submitted that claims 1-6, 8-14 and 17-22 are patentable over the cited reference(s) for the foregoing reasons.

CLAIMS 15-16

Claims 15 and 16 stand rejected as being unpatentable over Burns in view of Flyntz in view of Boyce and further in view of Tomat [USP 6,459,499]. Applicants respectfully traverse as discussed below. Because claims were amended in the instant amendment, the following discussion refers to the language of the amended claims. However, only those amended features

specifically relied upon to distinguish the claimed invention from the cited prior art shall be considered as being made to overcome the cited reference.

Each of claims 15-16 depends (directly or ultimately) from claim 1. Thus, each of claims 15 and 16 are considered to be allowable at least because of their dependency from an allowable base claim. This shall not; however, be considered an admission that claims 15-16 are not separately patentable from the identified combination of references.

It is respectfully submitted that claims 15 and 16 are patentable over the cited reference(s) for the foregoing reasons.

As provided by the Federal Circuit, a prior art reference can be combined or modified to reject claims as obvious as long as there is a reasonable expectation of success. *In re Merck & Co., Inc.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 19866). Additionally, it also has been held that if the proposed modification or combination would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious. Further, the teaching or suggestion to make the claimed combination and the reasonable suggestion of success must both be found in the prior art, not in applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). As can be seen from the forgoing discussion regarding the disclosures of the cited references, there is no reasonable expectation of success provided in the references that the suggested modification would be reasonably successful. Also, it is clear from the foregoing discussion a modification to the system described in Burns would change the principle of operation of the system and methodology described in Burns.

It is respectfully submitted that claims 1-6, and 8-22 are patentable over the cited reference(s) for the foregoing reasons.

It is respectfully submitted that the subject application is in a condition for allowance. Early and favorable action is requested.

Applicants believe that additional fees are not required for consideration of the within Response. However, if for any reason a fee is required, a fee paid is inadequate or credit is owed for any excess fee paid, the Commissioner is hereby authorized and requested to charge Deposit Account No. **04-1105**.

Respectfully submitted,
Edwards Angell Palmer & Dodge, LLP

Date: March 18, 2009

By: / William J. Daley, Jr. /

William J. Daley, Jr.
(Reg. No. 35,487)
P.O. Box 55874
Boston, MA 02205
(617) 239-0100

Customer No. 21,874